citizens. A basic precondition for this cooperation is a clear legal and public policy framework for action.

Businesses also need protection from unnecessary restrictions placed by federal and state antitrust laws on critical information sharing that would inhibit identification of R&D needs or the identification and mitigation of vulnerabilities. There are a number of precedents for this kind of collaboration, and we believe that legislation based on these precedents will also assist this process.

Faced with the prospect of unintended liabilities, we also believe that any assurances that Congress can provide to companies voluntarily collaborating with the government in risk management planning activity—such as performing risk assessments, testing infrastructure security, or sharing certain threat and vulnerability information—will be very beneficial. Establishing liability safeguards to encourage the sharing of threat and vulnerability information will add to the robustness of the partnership and the significance of the information shared.

Thank you for considering our views on this important subject. We think that such legislation will contribute to the success of the institutional, information-sharing, technological, and collaborative strategies outlined in Presidential Decision Directive—63 and version 1.0 of the National Plan for Information Systems Protection.

Sincerely,

Americans for Computer Privacy.
Edison Electric Institute.
Fannie Mae.
Internet Security Alliance.
Information Technology Association of America.
Microsoft.
National Center for Technology and Law, George Mason University.
Owest Communications.
Security.
Computer Sciences Corporation.
Electronic Industries Alliance.
The Financial Services Roundtable.
Internet Security Systems.
National Association of Manufacturers.
Mitretek Systems.
The Open Group.
Oracle.
U.S. Chamber of Commerce.

WHY INFORMATION SHARING IS ESSENTIAL FOR CRITICAL INFRASTRUCTURE PROTECTION

FREQUENTLY ASKED QUESTIONS

What are Critical Infrastructures?

Critical Infrastructures are those industries identified in Presidential Decision Directive—63 and version 1.0 of the National Plan for Information Systems Protection, deemed vital for the continuing functioning of the essential services of the United States. These include telecommunications, information technology, financial services, oil, water, gas, electric energy, health services, transportation, and emergency services.

What Is the Problem?

90% of the nation's critical infrastructures are owned and/or operated by the private sector. Increasingly, they are inter-connected through networks. This has made them more efficient, but it has also increased the vulnerability of multiple sectors of the economy to attacks on particular infrastructures. According to the Carnegie-Mellon Computer Emergency Response Team (CERT), cyber attacks on critical infrastructures have grown at an exponential rate over the past three years. This trend is expected to continue for the foreseeable future. In our free market system, it is not feasible to have a centralized-government monitoring function. A voluntary national industry-government information sharing system is needed in order for the nation to create an effective early warning system, find and fix vulnerabilities, benchmark best practices and create new safety technologies.

How Do Industries and the Government Share Information?

Based on PDD–63 and the National Plan, a number of organizations have been created to foster industry-government cooperation. These include Information Sharing and Analysis Centers (ISACs). ISACs are industry-specific and have been set up in the financial services, telecommunications, IT, and electric energy industries. Others are in the process of being organized. ISACs vary in their membership structures and relationship to the government. Most of them have a formal government sector liaison as their principal point of contact.

What Are Current Concerns?

Companies are concerned that information voluntarily shared with the government that reports on or concerns corporate security may be subject to FOIA. They are also concerned that lead agencies may not be able to effectively control the use or dissemination of sensitive information because of similar legal requirements. Access to sensitive information may fall into the hands of terrorists, criminals, and other individuals and organizations capable of exploiting vulnerabilities and harming the U.S. Unfiltered, unmediated information may be misinterpreted by the public and undermine public confidence in the country's critical infrastructures. Also, competitors and others may use that information to the detriment of a reporting company, or as the basis for litigation. Any and all of these possibilities are reasons why the current flow of voluntary data is minimal.

What Can Be Done?

Possible solutions include creating an additional exemption to current FOIA laws. There are currently over 80 specific FOIA Exemptions throughout the body of U.S. law, so it is clear that exempting voluntarily shared information that could affect national security is consistent with the intent and application of FOIA. Another solution is to build on existing relevant legal precedents such as the 1998 Y2K Information and Readiness Disclosure Act, the 1984 National Cooperative Research Act, territorially limited court rulings, and individual, advisory Department of Justice Findings.

Why Pursue a Legislative Solution?

The goal is to provide incentives for voluntary information sharing. Legislation can add legal clarity that will provide one such incentive, as well as also demonstrate the support and commitment of Congress to increasing critical infrastructure assurance.

PERSONAL EXPLANATION

HON. SHELLEY BERKLEY

OF NEVADA

IN THE HOUSE OF REPRESENTATIVES

Tuesday, July 10, 2001

Ms. BERKLEY. Mr. Speaker, flight delays caused me to miss rollcall votes Nos. 186, 187, and 188. Had I been present, I would have voted "yes" on No. 186, "yes" on No. 187, and "yes" on No. 188.

CELEBRATING THE DEFENSE LOGISTICS AGENCY'S 40TH ANNIVERSARY

HON. JAMES P. MORAN

OF VIRGINIA

IN THE HOUSE OF REPRESENTATIVES

Tuesday, July 10, 2001

Mr. MORAN of Virginia. Mr. Speaker, I rise today to congratulate the Defense Logistics Agency's 40th anniversary. The Defense Logistics Agency has a distinguished history as the nation's combat support agency. Its origins date back to World War II when America's entrance into the global conflict required the rapid procurement of large amounts of munitions and supplies. When the agency was first founded, managers were appointed from each branch of the armed services for this task. In 1961, the Department of Defense centralized management of military logistics support by establishing the Defense Supply Agency. After 16 years of increasing responsibilities, the Defense Supply Agency expanded its original charter and was renamed the Defense Logistics Agency in 1977.

I would like to commend the Defense Logistics Agency's impeccable record of supporting defense and humanitarian missions. It stands as a testament to the agency's commitment to provide seamless support of our armed forces around the world and to extend a helping hand to victims of all types of adversity.

As the world has changed and evolved, the Defense Logistics Agency also has adapted and proven its ability to streamline. Agency employees have shown dedication to improving quality, reducing costs and improving responsiveness to their warfighter customer needs. They have also demonstrated their ability to embrace the latest technologies of today's competitive business world, which has resulted in saving the taxpayers billions of dollars. The Defense Logistics Agency's record of achievement serves as an example of government service at its best, highlighted by two Joint Meritorious Service Awards.

On behalf of my colleagues, I would like to praise the individual efforts of the men and women involved in the Defense Logistics Agency, and thank them for making the Agency a world-class organization. In honor of the 40th anniversary of the Defense Logistics Agency, we are proud of the Defense Logistics Agency's past endeavors and look forward to a bright and successful future of continued commitment and service to our nation.

Mr. Speaker, I ask you to join me in extending congratulations and best wishes to the employees of the Defense Logistics Agency on this memorable occasion and achievement.

TRIBUTE TO JAMES H. MULLEN

HON. MARION BERRY

OF ARKANSAS

IN THE HOUSE OF REPRESENTATIVES

Tuesday, July 10, 2001

Mr. BERRY. Mr. Speaker, I rise today to pay tribute to a great Arkansan and outstanding educator. I am proud to recognize James H. Mullen in the Congress for his invaluable contributions and service to his community, to our state, and to our nation.